配置告警

Cisco Secure Workload 中的警报有助于监控工作负载安全并响应潜在威胁。警报的各个组件协同工作，提供可视性、警报源和配置，以及从发布服务器发送警报的功能。您可以配置警报，查看警报触发规则，并选择要发送警报的发布服务器。配置页面上显示的警报会因用户角色而异。警报发布服务器可以是警报或通知者。

注释 从 Cisco Secure Workload 3.0 版本开始，Cisco Secure WorkloadApp Store 不再支持警报和合规性应用。您可以在此页面上配置警报和合规性警报，而无需创建警报应用实例或合规性应用实例。

警报类型和发布服务器

Cisco Secure Workload 中的警报包括以下组件：

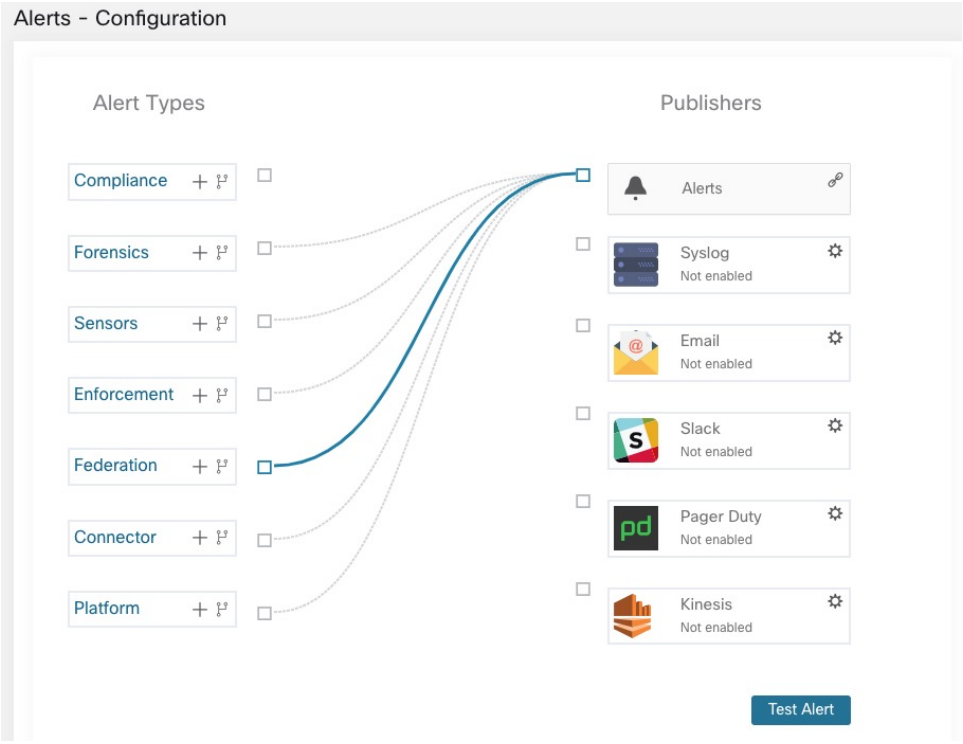
- **警报可视性**
  - **当前警报**：从导航窗格中，选择**调查 (Investigate)** > **警报 (Alerts)**。警报预览将发送到数据分流。
- **警报源和配置**：
  - **警报 - 配置**：从导航窗格中，选择**管理 (Manage)** > **工作负载 (Workloads)** > **警报配置 (Alert Configs)**。系统会显示使用通用模式和警报发布服务器配置的警报配置，以及通知程序设置。
- **发送警报**:

- **警报应用**：一种将生成的警报发送到已配置的数据分流的隐式 Cisco Secure Workload 应用。警报应用处理**暂停**和**取消**等功能。
- **警报发布服务器**：限制显示的警报数量，并将警报推送到 Kafka（MDT 或 DataTap）以供外部使用。
- **边缘设备**：将警报推送到其他系统，例如 Slack、PagerDuty、邮件等。

创建警报

要创建警报或触发规则，请从导航窗格中选择**警报 (Alerts)** > **配置 (Configuration)**：

Figure 1: 创建警报或触发规则



- **执行警报**
  - 代理可访问性
  - 工作负载防火墙
  - 工作负载策略
- **传感器警报**
  - 代理升级

- 代理流导出
- 代理签入
- 代理内存使用率
- 代理 CPU 配额
- 流观察结果的数量
- 已注册的新代理
- Pcap 状态
- 已卸载的代理
- 不推荐使用的密码
- 弃用的 TLS 版本
- 代理自动删除

- **合规性警报**
  - 执行策略
  - 实时分析策略

Note

- 对于执行和传感器警报类型，警报触发规则在当前选择的根范围内执行。
- 要为合规性警报类型创建警报触发规则，您必须在当前选择的范围内具有已执行的功能。

以下警报类型没有配置模式：

- 取证
- 连接器
- 联合
- Admiral
- 流量

交通警报

您可以创建**流量**警报，以便在工作负载与已知恶意 IPv4 地址通信时收到通知。默认情况下，用于检测恶意地址的选项已被禁用。要启用该选项以检测恶意地址，请参阅恶意 IPv4 地址的可视性。

可用的警报条件包括：

- **观察到恶意流 (Malicious flows are Observed)**：观察到与已知恶意 IPv4 地址的通信。

- **允许恶意流 (Malicious flows are Permitted)**：在策略分析和执行后，此条件会通知允许的恶意流。
- **拒绝恶意流 (Malicious flows are Rejected)**：在策略分析和执行后，此条件通知有关被拒绝的恶意流。

警报配置模式

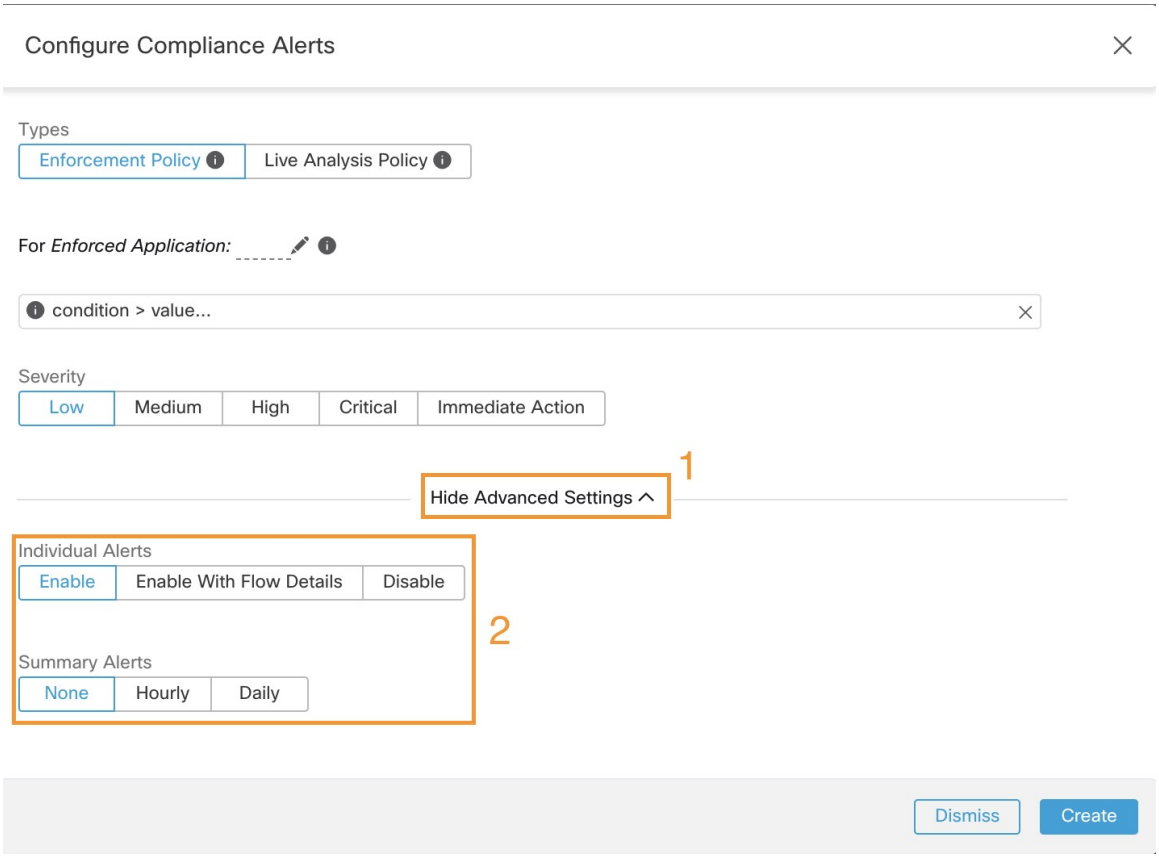
“警报配置”模式包含以下部分：

- 当警报配置因主题而异时，会显示警报类型

Note 邻域警报的警报类型不适用于 Cisco Secure Workload 3.7 及更早版本。

- 警报的主题。主题取决于应用，当警报模式是上下文模式时，可能会预先填入主题。
- 触发警报：“我们何时生成警报”(when will we generate an alert)。将鼠标悬停在  图标上以查找可用条件的列表。列表将显示特定于配置警报类型的可用条件。
- 警报严重性：如果生成了许多警报，则优先显示严重性较高的警报，而不显示严重性较低的警报。
- “摘要警报”(Summary Alert) 选项的配置选项。点击**显示高级设置 (Show Advanced Settings)**以展开。
- 关闭模式：如果要添加新警报并指定所有配置选项，请使用**创建 (Create)**；如果不添加任何新警报，请使用**消除 (Dismiss)**。

Figure 2: 警报配置模式高级选项



摘要警报

汇总警报仅适用于某些应用，以及取决于应用的某些配置选项。

- **单个警报**是基于非汇总或最低限度汇总的信息生成的，并且可能具有一分钟的时间范围。请注意，这并不一定意味着实际上会以分钟间隔生成和发送警报；也可以在应用频率间隔生成单个警报。
- 根据配置的警报规则（每小时或每天）为所有代理生成**汇总警报**。例如，系统会为代理汇总传感器和执行警报，并针对已配置的警报规则的所有流汇总合规性警报。

应用	应用频率 1	单个警报	每小时警报	每日警报
合规性	分钟	按应用频率	单个警报的摘要	单个警报的摘要
执行	分钟	按应用频率	单个警报的摘要	单个警报的摘要
传感器	分钟	按应用频率	单个警报的摘要	单个警报的摘要

Note 摘要警报的**事件时间**表示过去一小时或指定间隔内首次出现的相同警报类型。

暂停和取消警报

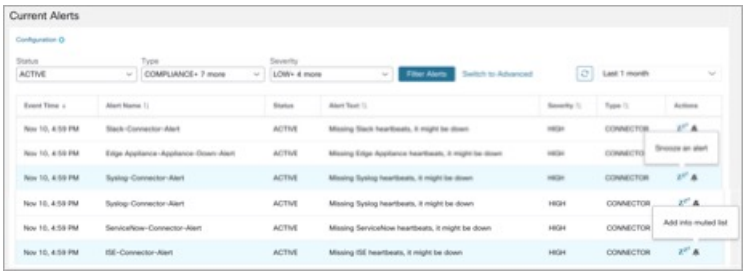
警报应用允许同一类型的警报在选定的时间内处于暂停状态。警报类型会有不同的定义，具体取决于当前配置的警报工作空间。例如，合规性警报类型定义为四个元组：使用者范围、提供者范围、协议和提供者端口。

Note 目前，您无法暂停或取消用户应用创建的警报。

要暂停警报，请执行以下操作：

1. 在**操作 (Actions)** 下，点击**暂停 (Snooze)** 图标。
2. 从“间隔”(Interval) 下拉列表中选择适当的间隔。
3. 点击**暂停 (Snooze)**。

Figure 3: 当前警报



要取消警报，请执行以下操作：

使用“取消”(Mute) 选项停止接收警报：

1. 在**操作 (Actions)** 下，点击**取消 (Mute)** 图标。
2. 要进行确认，请点击**是 (Yes)**。
3. （可选）要恢复警报，请从已取消列表中删除警报。（使用**状态 (Status)** 过滤器下拉列表查看所有**已取消 (MUTED)** 警报。）
4. 要恢复警报，请从已取消列表中删除警报。使用**状态 (Status)** 过滤器下拉列表查看所有**已取消 (MUTED)** 警报，然后恢复所需的警报。

Note 在一个范围内，您最多可以查看 5000 个已取消或暂停的警报。

Admiral 警报

Admiral 是一个集成的警报系统，用于取代早期版本中的 Bosun。有关详细信息，请参阅 Admiral 警报。

汇总与暂停

警报汇总适用于基于警报配置的所有主机，而暂停则适用于特定警报。

以下是两者之间的一些差异：

- 例如，合规性配置取决于应用工作空间以及应生成警报的违规类型。因此，汇总适用于基于警报规则的所有主机，例如转义条件，而暂停适用于非常特定的使用者范围、提供者范围、提供者端口、协议和转义条件。
- 按指定频率生成摘要警报，并包含在该间隔内生成的警报。摘要警报提供在指定频率间隔内触发的警报数量，以及该范围内所有代理的摘要。
- 只有在等待时间结束后产生新警报时，才会发送警报。此外，如果在源范围和目标范围之间的路径上配置了平台警报，且跳数小于一定数量，则会生成非常具体的警报。

Cisco Secure Workload 警报通知程序 (TAN)

Note 从 Cisco Secure Workload 版本 3.3.1.x 开始，TAN 将迁移到 **Cisco Secure Workload 边缘设备**。

警报通知程序提供通过各种工具（例如 Amazon Kinesis、邮件、系统日志和当前所选范围内的 Slack）发送警报的功能。作为范围所有者或站点管理员，可以为每个通知程序配置所需的凭证和通知程序应用的其他特定信息。

配置通知程序

要配置通知程序，您必须配置与警报相关的连接器。只能在部署 Cisco Secure Workload 边缘设备后配置连接器。有关部署 Cisco Secure Workload 边缘设备的详细信息，请参阅连接器的虚拟设备。

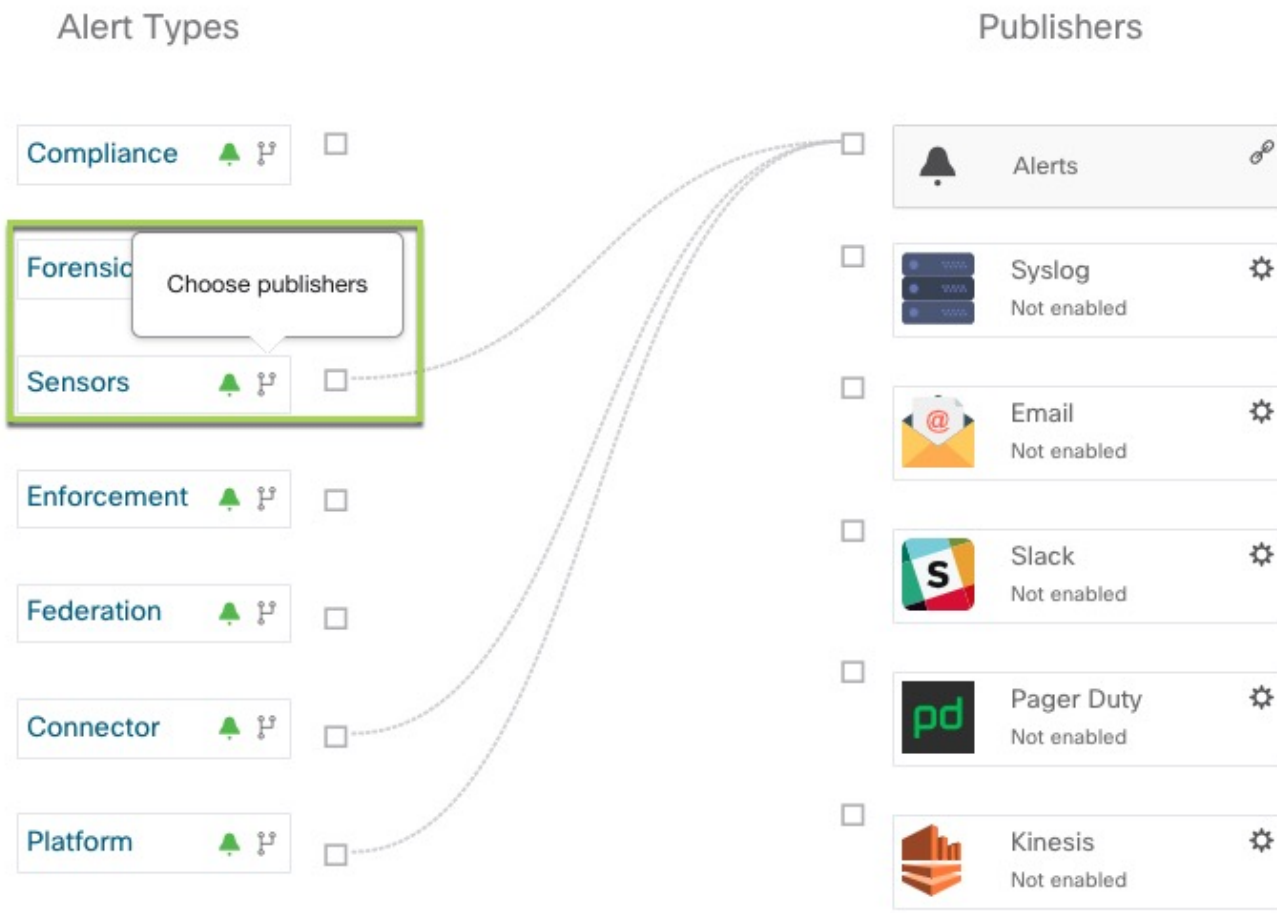
在设置 Cisco Secure Workload 边缘设备后，您可以使用其特定的所需输入来配置每个通知程序。设置 Cisco Secure Workload 边缘设备后，您将能够看到将警报类型连接到警报发布服务器的虚线。这是因为通知程序基于警报发布服务器构建。

应用频率是指应用运行和生成警报的大致频率。例如，“合规性”具有灵活的运行频率，实际上可能会在几分钟内计算警报。

选择警报发布服务器

范围所有者和**站点管理员**可以选择要**发送**警报的**发布服务器**。**发布服务器**包括 Kafka（数据分流）和**通知程序**。

Figure 4: 选择警报发布服务器



所有可用发布服务器都显示在**警报 - 配置 (Alerts - Configuration)** 窗口中，包括**警报 (Alerts)** 和 **活动通知程序 (Active Notifiers)**。您可以切换**发送**图标以选择警报类型的**发布服务器**。**最低警报严重性**是指警报必须达到的严重性级别才能通过**发布服务器**发送。

Note 选择外部数据分流可能会影响可以处理的最大警报数量。每分钟批处理的警报数量最多可减少到 14000 个。

外部系统日志隧道移至 TAN

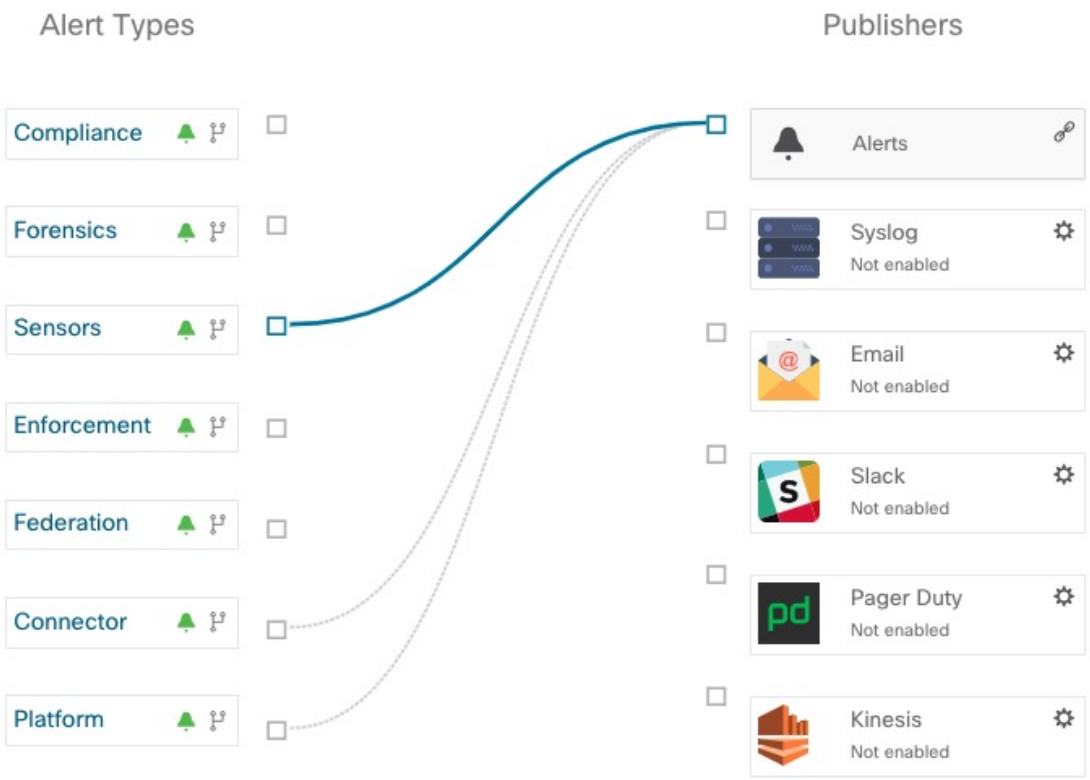
Note 从 3.1.1.x 版本开始，系统日志隧道功能将移至 TAN。要配置系统日志以获取平台级别系统日志事件，您必须在默认根范围内的 Cisco Secure Workload 边缘设备上配置 TAN。在默认根范围内配置 Cisco Secure Workload 边缘设备后，您可以设置系统日志服务器。要启用平台警报，请为平台启用系统日志通知。这可以通过启用“平台系统日志”连接来完成。

有关如何配置系统日志的详细信息，请参阅系统日志连接器。

连接图

连接图表显示**警报类型**和**发布服务器**之间的连接。为警报类型选择发布服务器后，系统会在警报类型和发布服务器之间建立一条蓝线。请注意，指向内部Kafka（数据分流）的线始终是用破折号创建的线，因为它表示构建警报通知的内部机制。

Figure 5: 连接图

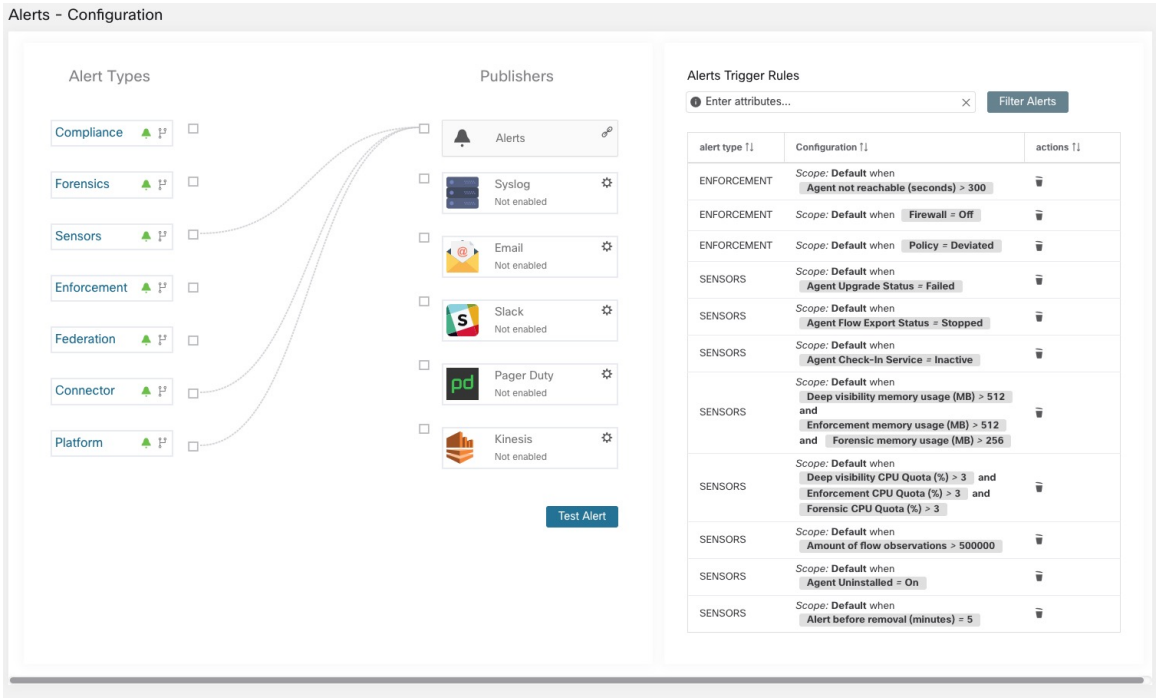


Note 用户应用生成的警报不会显示在“警报配置”(Alert Configuration) 页面中。用户应用能够向任何已配置的数据分流发送消息和警报。

查看警报触发规则

您可以在**警报 - 配置 (Alerts - Configuration)** 页面上查看所有已配置的警报触发规则的列表。您还可以执行以下任务：

Figure 6: 查看警报触发规则



“警报触发规则”窗口用于按警报类型和触发条件来过滤警报触发规则。

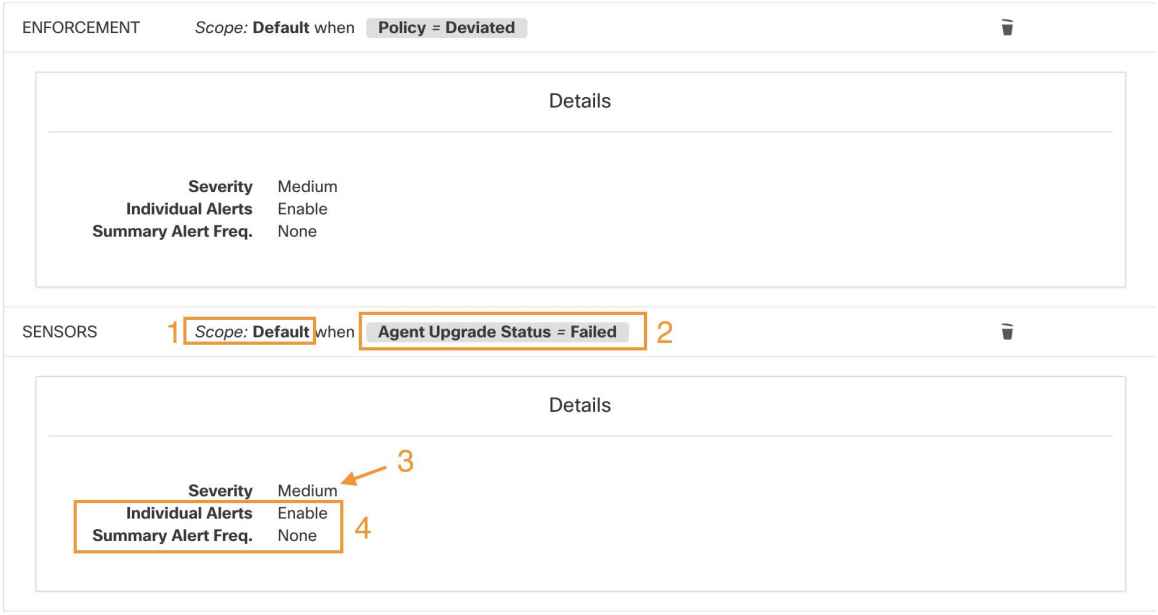
Note 警报触发条件是完全匹配条件。

警报触发规则详细信息

点击**警报触发规则 (Alerts Trigger Rules)** 部分中的一行以查看配置详细信息。

您还可以查看其他详细信息，例如**严重性 (Severity)**、**单个警报 (Individual Alerts)** 和**摘要警报频率 (Summary Alert Frequency)**。

Figure 7: 展开的警报配置



生成测试警报

生成测试警报的主要用途是验证与发布服务器的连接。您可以配置测试警报，以根据警报配置中的警报类型和链接发布服务器发送警报。

注释

- 生成测试警报并非来自实际源，仅为测试目的而生成。
- 可以为链接到至少一个发布服务器的警报类型生成测试警报。

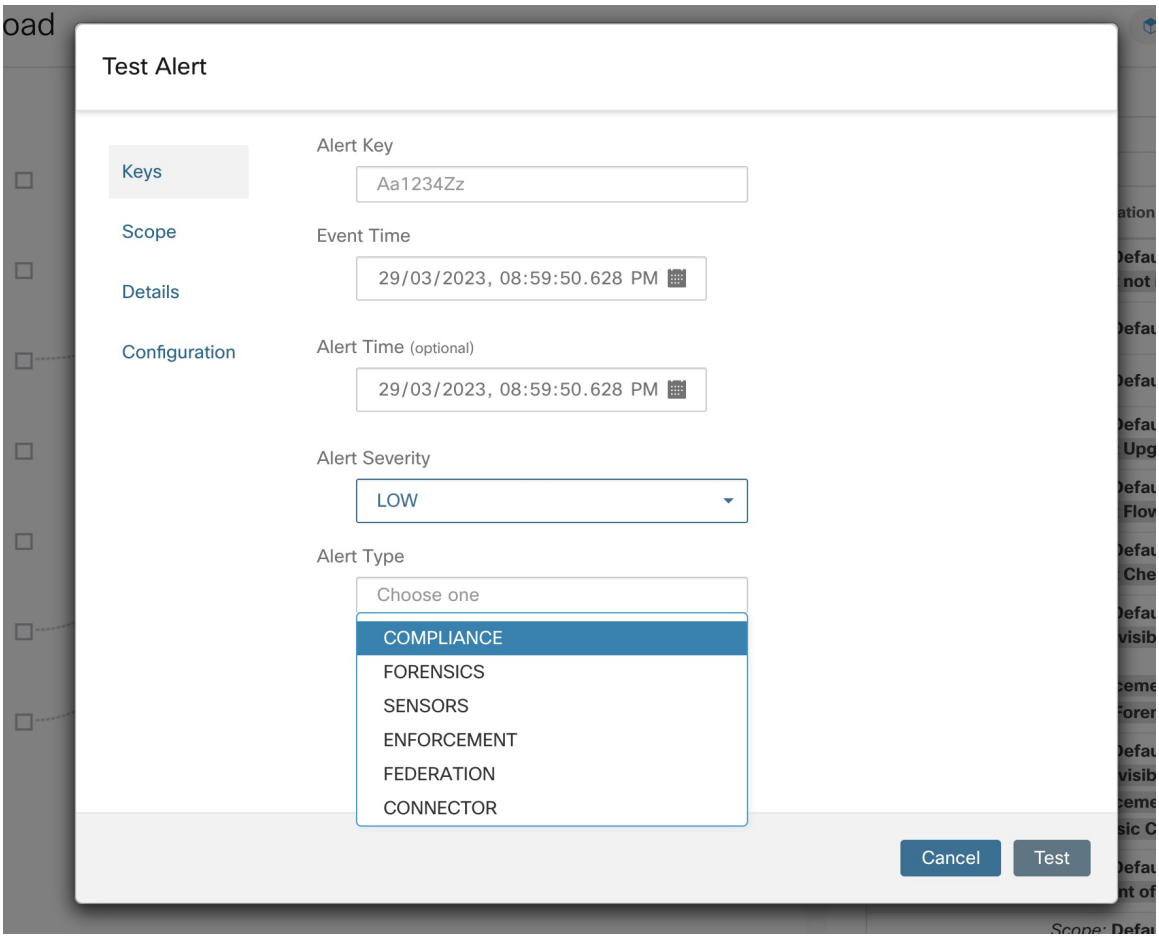
要生成测试警报，请执行以下步骤：

过程

步骤 1 从导航窗格中，选择**管理 (Manage)** > **工作负载 (Workloads)** > **警报配置 (Alerts Config)**。

步骤 2 要配置测试警报，请点击**测试警报 (Test Alert)**。

图 *8:* 测试警报配置



步骤 3 在**密钥 (Keys)** 选项卡下，输入“警报密钥”(Alert Key) 的值，然后选择“事件时间”(Event Time)、“警报时间”(Alert Time)、“警报严重性”(Alert Severity) 和“警报类型”(Alert Type) 的值。

步骤 4 在**范围 (Scope)** 选项卡下，“范围 ID”(Scope ID) 和“租户 ID”(Tenant ID) 的值会根据当前范围自动生成。

注释 如果租户 ID 与租户 ID VRF 相同，则系统会自动选中“租户 ID VRF”(Tenant ID VRF) 复选框。

步骤 5 在**详细信息 (Details)** 选项卡下，输入“警报文本”(Alert Text)、“事件注释”(Event Notes)、“警报详细信息”(Alert Details) 和“警报配置 ID”(Alert Configuration ID) 的值。

注释 “警报详细信息”(Alert Details) 可以是字符串或 JSON 格式的数据。

JSON 内容的选项包括：

1. 包含该警报类型所需的字段。
2. 任何示例 JSON 数据（如果该警报类型不需要默认 JSON 字段）。

   示例 JSON：

```
{"alert_name ":"sample","alert_category":{"severity": "dummy"}}
```

步骤 6 在**配置 (Configuration)**选项卡下，选择“单个警报”(Individual Alert)、“警报频率”(Alert Frequency) 和“汇总警报频率”(Summary Alert Frequency) 值。

对于单个警报，请从下拉列表中选择启用 *(ENABLE)* 或禁用 *(DISABLE)*。

系统自动选择警报频率，其中频率为单个 *(INDIVIDUAL)*。

注释 它仅支持单个警报，不会考虑汇总。

摘要警报自动选择为无 *(NONE)*。

步骤 7 要生成测试警报，请点击**测试 (TEST)**。

注释 系统将生成测试警报并将其发送到配置的发布服务器。

当前警报

导航至**调查 (Investigate)** > **警报 (Alerts)** 页面，查看所有活动警报的列表。您可以按**状态 (Status)**、**类型 (Type)**、**严重性 (Severity)** 和时间范围来过滤警报。

当前警报 (Current Alerts) 页面上仅显示严重性设置为 IMMEDIATE_ACTION、CRITICAL、HIGH、MEDIUM 或 LOW 的警报。无论严重性值如何，所有警报都将发送到配置的 Kafka 代理。

按时间范围过滤警报

1. 从下拉列表中选择一个范围。默认值为 1 个月。
2. 点击**自定义 (Custom)**并填写**开始 (From)** 和**结束 (To)** 日期以配置自定义范围。点击**应用 (Apply)**。请注意，当选择自定义时间范围时，**刷新**按钮将处于禁用状态。

高级过滤器

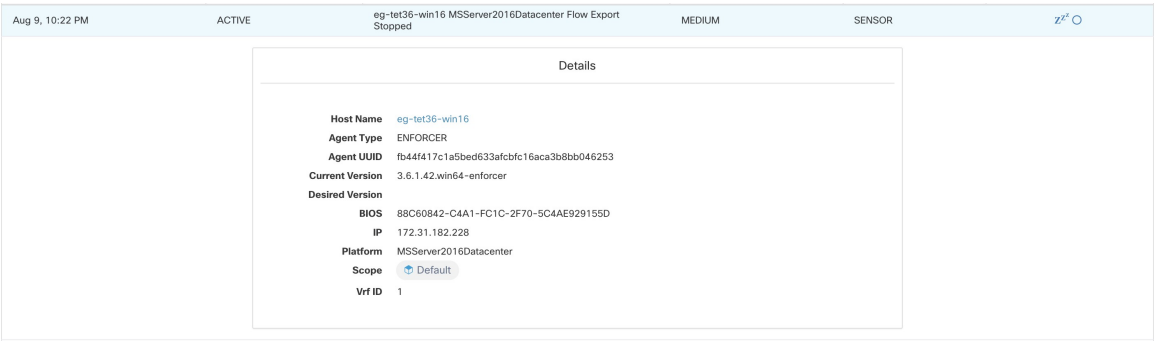
1. 点击**切换为高级 (Switch to Advanced)**。
2. 输入要过滤的属性。将鼠标悬停在**信息**图标上可查看要过滤的属性。

   当您切换回基本选项时，不会保留警报过滤器。

查看其他警报详细信息

您可以通过点击相应警报来查看有关警报的更多详细信息。

Figure 9: 警报详细信息



- 每个根范围每分钟只会显示 60 个警报。
- 警报数量越大，系统会生成称为**摘要警报**的警报类型，其中不会显示警报计数。
- 在任何时间点显示的警报都有最大数量限制；随着新警报的出现，系统会丢弃较旧的警报。有关详细信息，请参阅限制。

警报详细信息

常见警报结构

所有警报都遵循整体通用结构。结构对应于可通过 Kafka DataTaps 获得的 json 消息结构。

字段	格式	关于
root_scope_id	字符串	与范围层次结构中的顶级范围对应的范围 ID。
key_id	字符串	ID 字段，用于确定“类似”警报。相同的 key_id 会被暂停。
type	字符串	警报的类型。固定的字符串值集：COMPLIANCE、USERAPP、FORENSICS、ENFORCEMENT、SENSOR、PLATFORM、FEDERATION、CONNECTOR
event_time	长度	事件触发时的时间戳（如果事件跨越一个范围，则为该范围的起始时间）。此时间戳以纪元毫秒 (UTC) 为单位。

字段	格式	关于
alert_time	长度	首次尝试发送警报的时间戳。这将在事件的时间范围之后。此时间戳以纪元毫秒 (UTC) 为单位。
alert_text	字符串	警报的标题。
alert_text_with_names	字符串	内容与 alert_text 相同，但所有 id 字段均用相应名称代替。并非所有警报都存在此字段。
severity	字符串	固定字符串值集：LOW、MEDIUM、HIGH、CRITICAL、IMMEDIATE_ACTION。这是警报的严重性。对于某些类型的警报，这些值均可配置。
alert_notes	字符串	通常不设置。在某些特殊情况下可能存在，用于通过 Kafka DataTap 传递其他信息。
alert_conf_id	字符串	触发此警报的警报配置的 ID。可能并非所有警报都存在。
alert_details	字符串	结构化数据。字符串化的json。请参阅特定警报类型的功能详细信息，因为此字段的确切结构会因警报类型而异。
alert_details_json	json	与 alert_details 的内容相同，但未进行字符串化。仅针对合规性警报显示，并且仅可通过 Kafka 获得。
tenant_id	字符串	可能包含与 root_ scope_id 对应的 VRF。Or 可能包含 0 作为默认值。或者可能根本不存在。
alert_id	字符串	内部生成的临时ID。最好忽略。
alert_name	字符串	警报的名称。

- 合规性：lab-compliance-alert-details
- 取证：外部集成和取证事件字段
- 传感器：传感器警报详细信息
- 执行：执行警报详细信息

- 连接器：警报详细信息

本地集群的其他警报类型

- 交换矩阵：交换矩阵警报详细信息
- 联合：federation-alert-details
- 平台：警报详细信息
- 联合：federation-alert-details
- 平台：警报详细信息

通知程序的常规警报格式

以下示例说明了各种通知程序类型的警报显示方式。

Kafka (DataTaps)

Kafka (DataTap) 消息采用 JSON 格式。示例如下；有关其他示例，请参阅上面的 alert_details。


```
{
"_id" : ObjectId("66969d9b89f8901091b54f29"),
"key_id" : "SEN::6c12d5738f083632ad99acb1ba7a6dc4968938be-amt_of_flow_obs",
"event_time" : NumberLong("1721146728000"),
"alert_time" : NumberLong("1721146779640"),
"alert_text" : "Amount Of Flow Observed Above Threshold: collectorDatamover-2",
"alert_text_with_names" : "Amount Of Flow Observed Above Threshold: collectorDatamover-2",
"severity" : "HIGH",
"tenant_id" : "676767",
"root_scope_id" : "6666b8a9497d4f0a95461073",
"type" : "SENSOR",
"alert_details" : "{\"details\":{\"AgentType\":\"SENSOR\",\"Bios\":\"819FAC8D-39DE-
4C56-8CF4-7EEE25CF3510\",\"CurrentVersion\":\"3.10.2.26-
sensor\",\"DesiredVersion\":\"3.10.2.26-sensor\",\"HostName\":\"collectorDatamover-
2\",\"IP\":\"1.1.1.36\",\"LastConfigFetchAt\":\"2024-07-16 15:49:50 +0000
 UTC\",\"Platform\":\"CentOS-
7.9\"},\"agent_uuid\":\"6c12d5738f083632ad99acb1ba7a6dc4968938be\",\"scope_na
me\":\"Tetration\",\"scope_id\":\"6666b8a9497d4f0a95461073\",\"vrf_id\":676767,\"h
ost_name\":{\"collectorDatamover-
2\":\"6c12d5738f083632ad99acb1ba7a6dc4968938be\"},\"alert_sub_type\":[\"Amount
Of Flow Observed Above Threshold\"]}",
"alert_name" : "Amt_Of_Flow_Obs"
}
```


邮件

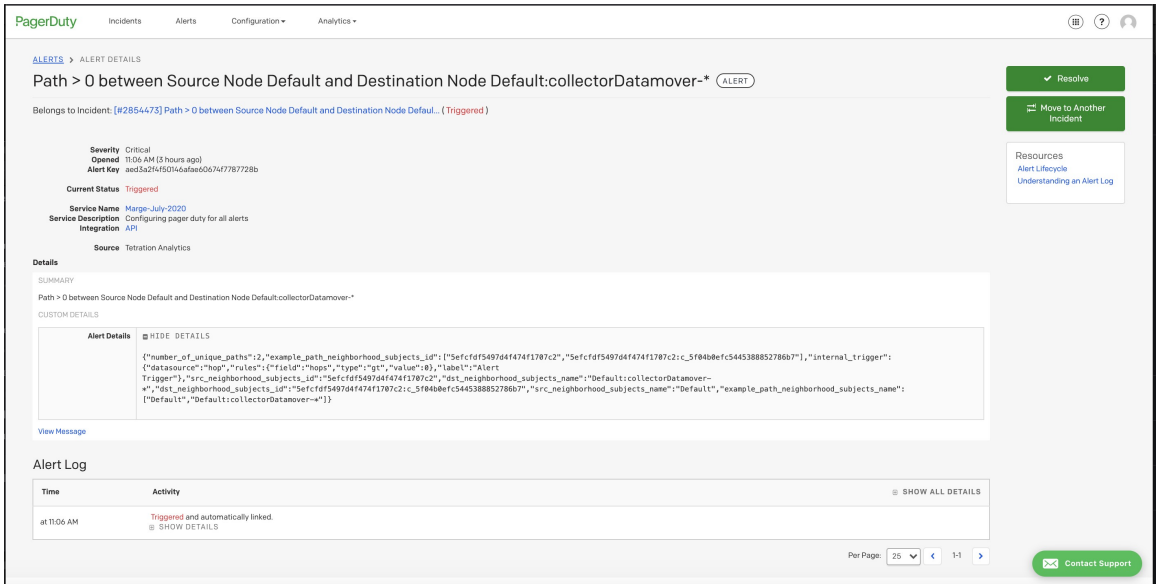
有关配置邮件警报的信息：邮件连接器

Figure 10: 思科 ***Cisco Secure Workload*** 警报的实例

PagerDuty

有关配置 PagerDuty 警报的信息：PagerDuty 连接器

Figure 11: PagerDuty 中的 ***Cisco Secure Workload*** 警报示例



发送到 PagerDuty 的警报是根据 key_id 重新触发的同一警报。

严重性会别映射到 PagerDuty 严重性，如下所示：

Cisco Secure Workload 严重性	PagerDuty 严重性
IMMEDIATE_ACTION	严重性
严重	严重性
高	错误
中	警告

Cisco Secure Workload 严重性	PagerDuty 严重性
LOW	信息

系统日志

有关配置系统日志警报和调整严重性映射的信息：系统日志连接器

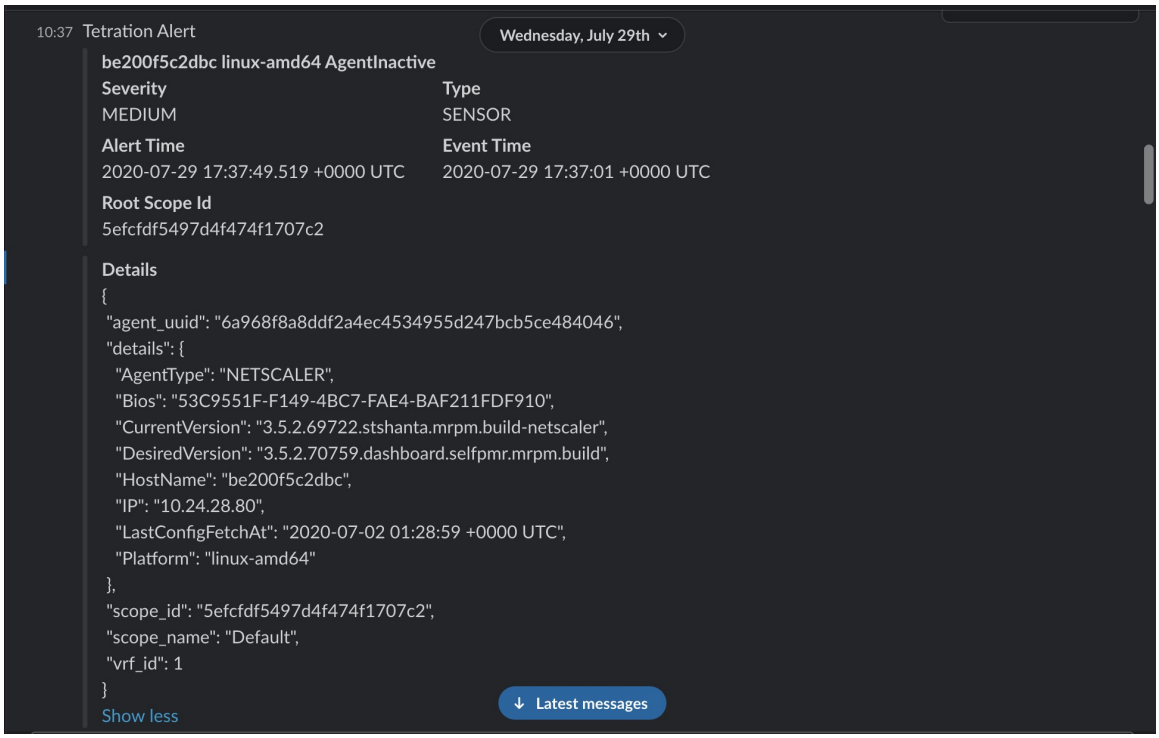
Figure 12: 发送到系统日志的 ***Cisco Secure Workload*** 警报示例


```
Aug  2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"3ee0d8b7-bc81-3427-9e84-6b9f8fedb98c","eventTime":"159639
3720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"L
OW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope
_names\":[\"Default\"],\"provider_port\":53,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":37367,\"protocol\":\"UDP\",\"co
nsumer_address\":\"172.31.163.139\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":39652,\"protocol\":\"UDP\",\"consumer_address\":
\"172.31.163.137\",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":63811,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.136\
",\"provider_address\":\"171.70.168.183\",\"provider_port\":53},{\"consumer_port\":57418,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.138\",\"provider_addr
ess\":\"173.36.131.10\",\"provider_port\":53},{\"consumer_port\":12599,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.141\",\"provider_address\":\"173.36.131
.10\",\"provider_port\":53},{\"consumer_port\":7385,\"protocol\":\"UDP\",\"consumer_address\":\"172.31.163.140\",\"provider_address\":\"173.36.131.10\",\"provider_po
rt\":53}],\"escaped_count\":6,\"provider_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"UDP\",\"internal_trigger\":{\"
datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596
393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"
Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug  2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"8f0cfcb5-f8c1-3130-a069-3721b7d50159","eventTime":"159639
3720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"L
OW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope
_names\":[\"Default\"],\"provider_port\":5660,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":17131,\"protocol\":\"TCP\",\"
consumer_address\":\"172.26.231.193\",\"provider_address\":\"172.31.163.140\",\"provider_port\":5660}],\"escaped_count\":1,\"provider_scope_ids\":[\"5efcfdf5497d4f47
4f1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"TCP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\
"type\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeI
d":"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1
"}
Aug  2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"1ef4a974-be89-31de-abe9-dc71cb0170ad","eventTime":"159639
3720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"L
OW","tenantId":"0","type":"COMPLIANCE","alertDetails":"{\"consumer_scope_ids\":[\"5efcfdf5497d4f474f1707c2\"],\"consumer_scope_names\":[\"Default\"],\"provider_scope
_names\":[\"Default\"],\"provider_port\":443,\"application_id\":\"5f04b0b9755f024d4e36a279\",\"constituent_flows\":[{\"consumer_port\":17792,\"protocol\":\"TCP\",\"c
onsumer_address\":\"172.26.231.193\",\"provider_address\":\"172.31.163.133\",\"provider_port\":443}],\"escaped_count\":1,\"provider_scope_ids\":[\"5efcfdf5497d4f474f
1707c2\"],\"policy_type\":\"ENFORCED_POLICY\",\"protocol\":\"TCP\",\"internal_trigger\":{\"datasource\":\"compliance\",\"rules\":{\"field\":\"policy_violations\",\"t
ype\":\"contains\",\"value\":\"escaped\"},\"label\":\"Alert Trigger\"},\"time_range\":[1596393720000,1596393779999],\"policy_category\":[\"ESCAPED\"]}","rootScopeId"
:"5efcfdf5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
```


Slack

有关配置 Slack 警报的信息：Slack 连接器

Figure 13: 发送到 ***Slack*** 信道的 ***Cisco Secure Workload*** 警报示例



Kinesis

有关配置 Kinesis 警报的信息：Kinesis 连接器

Kinesis 警报与 Kafka 警报类似，因为两者都是消息队列。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。